# Chapter Two : Reducing burdens on businesses and delivering better outcomes for people

Date – 17.12.21

## 2.1 Introduction

No questions

## 2.2 Reform of the accountability framework

### Q2.2.1. To what extent do you agree with the following statement: ‘The accountability framework as set out in current legislation should i) feature fewer prescriptive requirements, ii) be more flexible, and iii) be more risk-based’?

Somewhat Disagree

#### Q2.2.1a. Please explain your answer and provide supporting evidence where possible.

#### It is noted the similarity between the current accountability framework and the one proposed.

Organisations are only now getting to grips with the requirements of the accountability framework under the new regime which came into force in May 2018, and it would be unwise to change the current accountability framework for the proposed Privacy Management Programme just for the sake of making a cosmetic change.

It is noted that there is a lot of similarity between the content and requirements of the Privacy Management Programme set out in para 156 and the content and requirements of the current accountability framework under the UK GDPR. We would therefore argue that the proposed Privacy Management programme may come across as some of the existing requirements under the current accountability framework being re- worded or merged with other requirements. For example, there is very little difference between the contents of para 156 in the consultation paper and [what the ICO has identified in answer to the question “What do we need to do”](https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/#whatdo).

Clear prescriptive requirements have the following advantages

1. Support organisations in understanding what they need to do
2. Public have confidence in how their data is used

A risk-based approach is pragmatic and should be encouraged and strengthened. However, the overall approach could be undermined with a scaling back of the other elements, for example the removal of DPIAs as a statutory requirement.

Flexibility must be based on whether an organisation is carrying out high or low risk processing rather than the size of the organisation as many small organisations may carry out high risk processing. Flexibility based on any other approach other than a risk -based approach could be considered to reduce the importance of the current accountability framework of the proposed Privacy Management Programme. Some organisations may see this change as a ’get out of jail card’ for not having the correct policies and procedures in place in order to be able demonstrate to other organisations, relevant regulators and the public that they are compliant with the requirements under data protection legislation

In addition, organisations are just about getting to grips with the current accountability framework, and we believe it would be unwise to change again for something not dissimilar but with a different name which would lead to confusion.

### Q2.2.2.To what extent do you agree with the following statement: ‘Organisations will benefit from being required to develop and implement a risk-based privacy management programme’?

Neither Agree nor Disagree

#### Q2.2.2a. Please explain your answer, and provide supporting evidence where possible and in particular:

#### Whether a privacy management programme would help organisations to implement better, and more effective, privacy management processes.

#### Whether the privacy management programme requirement would risk creating additional burdens on organisations and, if so, how.

It has been noted above in our response to q 2.2.1 a) above that there the proposed Privacy Management Programme is broadly similar to the requirements under the current accountability framework. The proposed Privacy Management programme would pull everything together and perhaps bring about a wider understanding of requirements through organisations. It may also be an easier approach for those smaller organisations currently struggling to meet requirements. It is accepted that the Government should review the contents of the accountability framework/privacy management programme to ensure that the framework/programme moves away from box-ticking compliance and the contents are to the benefit of organisations and data subjects. Organisations should be able to take account of existing sector specific standards such as the NHS Data Security Protection Toolkit as a way of demonstrating that they are compliant with the proposed privacy management programme.

It has already been noted in the answer to Q. 2.2.1.a) above that organisations are only now getting to grips with the new accountability framework introduced under the UK GDPR in May 2018. In order to understand what needs to be in place under the new proposed privacy management programme more time/resources will be needed to understand the differences between the current accountability framework and the proposed PMP in order to comply with the new requirements.

The new privacy management programme must cover the same area as the accountability framework in order to maintain the current high standards of data protection for organisations and data subjects. A tiered approach based on the level of data protection risk rather than types of organisations would be useful.

### Q2.2.3. To what extent do you agree with the following statement: ‘Individuals (i.e., data subjects) will benefit from organisations being required to implement a risk-based privacy management programme’?

Somewhat Disagree

### Q2.2.4. To what extent do you agree with the following statement: ‘Under the current legislation, organisations are able to appoint a suitably independent data protection officer’?

No response.

#### Please explain your choice and provide supporting evidence where possible.

It has been noted above in our response to Q2.2.1.a that making a cosmetic name change from accountability framework to privacy management programme will not benefit individuals. The accountability framework or privacy management programme regardless of what it is called will only benefit individua’s data protection rights if it is properly implemented. The focus of any reforms to the current data protection legislation must be on implementation. If the proposed new privacy management programme reduces organisation’s obligations, then such a reduction will not benefit individuals. Individuals should already benefit from organisations being required to meet the accountability principle. We do not see how the new ‘reduced’ approach will add any increased benefit to individuals.

Individuals will only benefit if organisations undertake a risk-based assessment of their data processing activities. Once they have carried out the assessment, they must put in place policies and procedures to mitigate the risks which they have identified in their assessment. They also need to check that the policies and procedures are being followed correctly. Failure to carry out the risk assessment or to check that the policies and procedures are being followed correctly will have an impact on individual’s data protection rights.

Public sector organisations have a number of ways in which they can demonstrate compliance with the current accountability framework ranging from the NHS data Security and Protection Toolkit in the health and social care sector to the Asset Recovery Certification Scheme, the Age Check Certification Scheme and the Age-Appropriate Design Schemes – the last 3 mentioned approved by the ICO under the UK GDPR.

### **Q2.2.5. To what extent do you agree with the proposal to remove the existing requirement to designate a data protection officer?**

Somewhat Disagree.

#### Q2.2.5a. Please explain your answer and provide supporting evidence where possible.

he current requirement to appoint a Data Protection Officer (DPO) is working well and doesn’t need changing. The role of the Data Protection Officer (DPO) is now widely recognised within many organisations and individuals know to contact the DPO in an organisation as their first port of call if they want to make a data protection complaint or exercise their individual rights.

Changing the name of the postholder responsible for the tasks assigned to the DPO in the legislation could have negative impact on organisations. This is because it could create confusion. Firstly, with the public, as they would need to understand who it is they can contact to support them in exercising their information rights. Secondly within organisations, where individuals are currently aware of what a data protection officer is there to do, and the importance of contacting them in the event of an incident, or to seek advice on their processing of personal data. “Privacy Management Programme Lead” is a term that may only make sense to those who work within the field, whereas Data Protection Officer is clearly someone who can help in the field of data protection.

If the requirement to appoint a DPO were to be removed, allowing organisations to choose whether to appoint a DPO based on risk of processing activity would be sensible, but organisations would need guidance, or it should be explicit in the legislation on what factors need to be considered as part of the data protection risk assessment to determine whether the organisation needs to appoint a DPO. As before, this would only be effective if risks are assessed correctly, and this would require someone with data protection expertise to undertake in the first place.show

### Q2.2.6. Please share your views on whether organisations are likely to maintain a similar data protection officer role, if not mandated?

If organisations, such as SMEs in the private sector or small third sector organisations have incurred a cost in appointing a DPO, such as having an external DPO, then it is possible that these organisations may cease these arrangements if the requirement to appoint a DPO is not mandatory. This may lead to a reduction in data protection compliance in such organisations and individuals not being able to enforce their data protection rights. This may lead to greater pressure on the limited resources which the ICO has in its regulatory and enforcement teams.

However, participants from the VCSE sector in our Greater Manchester conversations about the consultation indicated that a number of organisations within the sector would maintain a lead for data protection, as they would be required to demonstrate compliance when bidding for work with local government or health partners for example.

In Local Authorities the existence of a Data Protection Officer has been the norm for several years, in the form of “Information Governance Managers”, and most of those within Greater Manchester simply experienced a formal change to or addition of “Data Protection Officer” to their job title. As a result, the likelihood is that these job titles would remain, to ensure continuity for the business and the public served by those authorities.

### **Q2.2.7. To what extent do you agree with the following statement: ‘Under the current legislation, data protection impact assessment requirements are helpful in the identification and minimisation of data protection risks to a project’?**

Strongly Agree

#### Q2.2.7a. Please explain your answer and provide supporting evidence where possible.

Data Protection Impact Assessments are a useful tool to assess the risks of new data processing activity to individuals, and provides members of staff responsible for data protection compliance with oversight of the planned activity. To produce a DPIA the business or service areas responsible for the new processing activity must work closely with staff responsible for data protection. This collaboration increases the data protection knowledge of the business or service areas since they must document in the DPIA how the new processing activity meets the data protection principles. Undertaking a DPIA also allows for the collection and completion of information needed for the ROPA.

### Q2.2.8. To what extent do you agree with the proposal to remove the requirement for organisations to undertake data protection impact assessments?

Strongly Disagree.

#### Q2.2.8a. Please explain your answer, and provide supporting evidence where possible, and in particular describe what alternative risk assessment tools would achieve the intended outcome of minimising data protection risks.

Although we agree that a what is included within a DPIA should be flexible and organisations should be able to decide what level a DPIA should be undertaken dependent on the risk involved, removing the need for clearly defined assessment from within legislation may lead to some organisations not undertaking any element of risk assessment, regardless of the expectations of the privacy management programme, which has the potential to place individual rights at risk.

Furthermore, many data protection professionals often face challenges within the organisations to ensure that data processing is documented, and risks are appropriately assessed and mitigated. Removal of the requirement for a DPIA completely would impact on their ability to drive this expectation within an organisation. Within the public sector, it has taken a long time to embed DPIA processes which were previously good practice under the Data Protection Act 1998. Following the statutory requirement being introduced under GDPR, non-information governance practitioners within the business now mostly understand what is required, and proactively seek support from Information Governance colleagues when embarking upon new projects. If the requirement to carry out DPIA’s was removed This would have an impact on data protection compliance within the public sector and ensuring that individual data protection rights were upheld within the sector.

The requirement to publish information from DPIAs may however increase the value of the work as they will inform the public and allow for knowledge sharing across organisations.

From the perspective of members of the public (as opposed to those working in the data protection field), participants in our Greater Manchester wide discussions felt that they did not know what the process of Data Protection Impact Assessment involved and were mostly not consulted in the process of the assessments being undertaken. It would be useful to strengthen this message via guidance etc. published by the ICO.

### **Q2.2.9. Please share your views on why few organisations approach the ICO for ‘prior consultation’ under Article 36 (1)-(3). As a reminder Article 36 (1)-(3) requires that, where an organisation has identified a high risk that cannot be mitigated, it must consult the ICO before starting the processing. Please explain your answer and provide supporting evidence where possible.**

Whilst it should be a rare occurrence for a processing activity to be high risk that cannot be mitigated. It is likely that those organisations that do approach the ICO are facing a challenge that a risk ‘will not’ be mitigated rather than it can’t be. It is expected that one of two scenarios currently occur:

* Organisations that are keen to manage risk will ensure that appropriate mitigation is in place
* Organisations that are not mitigating risks appropriately may consider the level of risk lower so that it falls outside Article 36 (1)-(3) or not engage in the risk assessment process and thus not involve the ICO

It is the experience of some GM organisations that where the assessment reveals there is a high risk from the proposed activity that cannot be mitigated, organisations may come to the view that the benefits of carrying out the high-risk activity are not as great as the risks and therefore abandon the project rather than consulting with the ICO under Article 36. Alternatively, the move to require consultation with the ICO often results in project teams and suppliers revisiting the risks to identify possible mitigations. One authority within Greater Manchester did consult the ICO on a project with unmitigated high risks, and the consultation resulted in the supplier bringing forward an upgrade which had previously been deemed not possible, in order to mitigate the risk and meet the terms of the contract they had with the organisation. As a result, during the ICO consultation period the risk was mitigated and so the finding from the ICO was purely in a review capacity and did not result in any recommendations for follow up.

In this case the ICO consultation was effective since it resulted in the supplier delivering a system which was compliant with data protection legislation despite the previous view of the supplier that it was not possible to bring the upgrade forward

### Q2.2.10. To what extent do you agree with the following statement: ‘Organisations are likely to approach the ICO before commencing high risk processing activities on a voluntary basis if this is taken into account as a mitigating factor during any future investigation or enforcement action’?

Neither Agree nor Disagree

#### Q2.2.10a. Please explain your answer, and provide supporting evidence where possible, and in particular:

#### What else could incentivise organisations to approach the ICO for advice regarding high-risk processing?

The Greater Manchester Local Authorities Information Governance Expert Reference Group, made up of information governance specialists from all the local authorities within Greater Manchester has often approached the ICO for advice on matters and have been successful in engaging with the ICO on matters such as Troubled Families, and local contact tracing during the Covid-19 pandemic. On occasion the ICO have not had the capacity to provide advice and guidance directly. The Government needs to ensure that the ICO is properly resourced, so that it can provide timely and appropriate advice to organisations on Article 36 issues.

The ICO has always taken a positive view of organisations voluntarily engaging with them. For example, the ICO guidance on audits suggests that if a breach were to be detected during a consensual audit, they would not necessarily take enforcement action, rather they would provide guidance on the steps to take to mitigate the breach.

As an example of how this might be improved, the use of Sandbox type support from the ICO for innovative but high-risk processing may also encourage organisations to approach the ICO.

### Q2.2.11. To what extent do you agree with the proposal to reduce the burden on organisations by removing the record keeping requirements under Article 30?

Neither Agree nor Disagree

#### Q2.2.11a. Please explain your answer and provide supporting evidence where possible.

The requirement to create and maintain a Register of Processing Activities (ROPA) leads to a significant volume of resource that is often very difficult to maintain, specifically across a large multi-functional organisation. The requirement for personal data inventories as part of the proposed Privacy Management   Programme (PMP) will likely require similar resource to meet similar challenges.  If the requirement for personal data inventories is introduced as part of the proposed PMP then it is logical to remove the Article 30 record keeping requirement.  If the PMP is not introduced, then the prescriptive elements of what must be included in the RoPA should be removed. If the RoPA is to fulfil its purpose, then it cannot be an unused spreadsheet and needs to be updated on a regular basis. The ICO needs to update its guidance on what should be included in a RoPA if the prescriptive elements are removed

### Q2.2.12. To what extent do you agree with the proposal to reduce burdens on organisations by adjusting the threshold for notifying personal data breaches to the ICO under Article 33?

Strongly Agree

#### Q2.2.12a. Please explain your answer, and provide supporting evidence where possible and in particular:

#### Would the adjustment provide a clear structure on when to report a breach?

#### Would the adjustment reduce burdens on organisations?

#### What impact would adjusting the threshold for breach reporting under Article 33 have on the rights and freedoms of data subjects?

The proposal seems similar to the approach taken currently by the ICO when advice is sought on what is a reportable personal data security breach. However, the recommendation to lower the threshold with clear guidance and potentially a risk template with thresholds to aid organisations in identifying whether the personal data breach requires notification to the ICO or not. The change would be unlikely to impact the rights and freedoms of data subjects, as organisations would still be under the obligation to record all personal data security breaches in a register even if the personal data security breach did not meet the new threshold for notification to the ICO.

### **Q2.2.13. To what extent do you agree with the proposal to introduce a voluntary undertakings process? As a reminder, in the event of an infringement, the proposed voluntary undertakings process would allow accountable organisations to provide the ICO with a remedial action plan and, provided that the plan meets certain criteria, the ICO could authorise the plan without taking any further action.**

Somewhat Agree

#### **Q2.2.13a. Please explain your answer and provide supporting evidence where possible.**

This is a good idea as it allows organisations to assess where shortcomings are in their data protection compliance (and in the process demonstrate that they understand their data protection risks) and propose a plan to improve compliance and prevent further infringements. This should reduce the burden on the ICO and result in better data protection compliance standards. Some organisations, in particular SMEs and small organisations in the charity and voluntary may need external help in putting a plan together to improve their data protection compliance and prevent further infringements which would impose a cost burden on them. We would like to see more information from the Government about their plans for the ICO to check that things are improving as planned, and what would the consequence be if no improvement was made?

### Q2.2.14. Please share your views on whether any other areas of the existing regime should be amended or repealed in order to support organisations implementing privacy management requirements.

* Consolidating UK GDPR and DPA 2018 into one piece of legislation.
* Producing guidance or a code of practice to make the exemptions in the DPA schedules clearer and easier to understand and apply for practitioners and data subjects.
* Legislation on rights of access to data relating to deceased persons, currently based on common law duty of confidentiality and limited case law, and specific legislation relating to health and social care records. (This could include revising the Access to Health Records legislation to cover social care records belonging to both Adults and Children’s services under DHSC and DfE oversight)
* Review of requirements around CCTV and in particular of body worn cameras taking into account recent case law.

### Q2.2.15. What, if any, safeguards should be put in place to mitigate any possible risks to data protection standards as a result of implementing a more flexible and risk-based approach to accountability through a privacy management programme?

* Clear detailed guidance on expectations as part of the privacy management programme on organisations
* Perhaps an annual return requirement similar to the DSP toolkit
* More advice and support to organisations on the changes to the privacy management programme
* Organisations should be encouraged to carry out Internal monitoring/analysis of complaints from data subjects as complaints provide a good indication of areas where improvements to data protection compliance may be needed
* Spot checks or audits from the ICO for all types of organisations.

#### Alt approach.

The questions below relate to alternative reform proposals should privacy management programmes not be introduced.

### Q2.2.16. To what extent do you agree that some elements of Article 30 are duplicative (for example, with Articles 13 and 14) or are disproportionately burdensome for organisations without clear benefits?

Strongly Agree

#### Q2.2.16a. Please explain your answer, and provide supporting evidence where possible, and in particular address which elements of Article 30 could be amended or repealed because they are duplicative and/or disproportionately burdensome for organisations without clear benefits.

A30(1) is duplicative of Articles 13 and 14. It is exceptionally time consuming to pull together into one document for a large organisation, and then even more difficult to maintain as an accurate record.

### Q2.2.17. To what extent do you agree that the proposal to amend the breach reporting requirement could be implemented without the implementation of the privacy management programme?

Strongly Agree

#### Q2.2.17a. Please explain your answer, and provide supporting evidence where possible

This would involve a change in the definition of a reportable personal data breach requiring notification to the ICO, which should be easy to do on a standalone basis.

### Q2.2.18. To what extent do you agree with the proposal to remove the requirement for all public authorities to appoint a data protection officer?

Somewhat Disagree

Q2.2.18a. Please explain your answer and provide supporting evidence where possible.

Having a DPO for public authorities which is required by law emphasises the value of that data and provides a contact person for individuals to be able to exercise their rights or raise concerns about the organisations personal data processing.

Public authorities need to be able to demonstrate the highest level of compliance in their processing of personal data in order that the public has the highest level of confidence in how their personal data is used at all levels of public service. Individual members of the public cannot choose their public authority as they can with organisations in the private sector. In the private sector organisations can chose an organisation in which they have trust and confidence that their personal data will be properly looked after. Small public authorities must demonstrate the same high level of data protection compliance as the large public authorities as the public expectation will not differ based on the size of the organisation, rather what the organisation is doing with personal data.

Data protection compliance breach by one public authority can have an impact on public confidence in the processing of personal data by other public authorities. As has been previously noted, ensuring the appropriate processes and practices are in place for accountability (under either the current regime or the new privacy management programme proposals) would require a postholder to manage this, and a Data Protection Officer would be the most appropriate role to do this, as they currently do.

### Q2.2.19. If you agree, please provide your view which of the two options presented at paragraph 184d(V) would best tackle the problem.

### Please provide supporting evidence where possible, and in particular:

### What risks and benefits you envisage

### What should be the criteria for determining which authorities should be required to appoint a data protection officer

N/A we do not agree with the proposal.

### Q2.2.20. If the privacy management programme requirement is not introduced, what other aspects of the current legislation would benefit from amendments, alongside the proposed reforms to record keeping, breach reporting requirements and data protection officers?

We have no further suggestions to add to answers provided earlier in this section.

## 2.3 Subject Access Requests

### Q2.3.1. Please share your views on the extent to which organisations find subject access requests time-consuming or costly to process.

Although the demands of any one request can vary, it is recognised that certain types of public services experience greater difficulty in completing requests and that they can be significantly time-consuming. Examples of this can be found within social care, where a combination of the volume/sensitivity of the information and the existing pressures faced by the workforce lead to this being a task that can often take a significant amount of time. Furthermore, requests that seek to collate all information held by an authority or copies of all emails regarding an individual can often be costly to process and take a significant amount of resource.

There is also sometimes the need to arrange support for the data subject when accessing the information, for example when it relates to social care records such as for Looked After Children or Adoption. Local Authorities also get a high number of SARs which are made prior to or during private legal proceedings. This can often be time consuming and in many instances costly in respect of the resource needed to handle the volume of requests received.

#### Q2.3.1a. Please provide supporting evidence where possible, including:

#### What characteristics of the subject access requests might generate or elevate costs

#### Whether vexatious subject access requests and/or repeat subject access requests from the same requester play a role

#### Whether it is clear what kind of information does and does not fall within scope when responding to a subject access request

For a local authority, which is a combination of multiple service areas delivering a wide array of public functions, requests which are not specific to a specific service area or particular type of records are problematic and difficult to manage. In addition, requests that seek copies of all correspondence (emails) where the data subject is referenced can also lead to a significant amount of resource needing to be allocated to review each item to see if it meets the scope of the request and make any required redactions.

Access to large social care files or for data held by departments where the subject has had a long history with the LA, and the complexity/sensitivity of the data held – requires consideration of exemptions and redaction process often by more than one department or case worker. Redaction is difficult and often inconsistent depending on who has carried it out.

The use of subject access from aggrieved individuals who repeatedly use the process to either cause a burden or seek to collate information to evidence a perceived failure is becoming an increasing burden on the organisation.  Requests that in effect circumvent court processes, e.g., both parents requesting child’s info in ongoing private family proceedings, or where contemplating litigation/in dispute with a service area e.g., planning, and requests for HR/Personnel files from employees/former employees as part of grievance processes. As data would be accessible through the processes to which they relate this is an additional burden for the organisation at a stage earlier that they would be prepared for. In addition, the results of these requests often mean that the individuals do not receive the information they are seeking, since it does not relate to themselves. In these cases, the request and the considerable work undertaken to meet the terms are wasted.

There are also grey areas which require a judgement call on what to include, e.g., where third party info and subjects’ data are entwined, or unsure of what is within subjects’ knowledge which would influence whether it’s reasonable to disclose data.

### Q2.3.2. To what extent do you agree with the following statement: ‘The ‘manifestly unfounded’ threshold to refuse a subject access request is too high’?

Somewhat Agree

#### Q2.3.2a. Please explain your answer, providing supporting evidence where possible, including on what, if any, measures would make it easier to assess an appropriate threshold.

A wider range of indicators may be beneficial. In addition, more guidance on what should be considered manifestly unfounded, particularly where the right is used as an alternative to the complaints system or alternative routes for dispute resolution.

Applicants with a prior adverse history with an organisation are still entitled to make valid requests and every request is considered on its own merit. It is hard to judge if a request is made to harass/cause disruption currently. Sometimes services will “know” the requestor is just being difficult on purpose (from the context of the information gathered in the process of the request, or the language used) but not always easy to fit into the criteria. It would be a good idea to include the requester’s ability or willingness to clarify their information request as a measure for assessing whether the request is manifestly unfounded.

### Q2.3.3. To what extent do you agree that introducing a cost limit and amending the threshold for response, akin to the Freedom of Information regime (detailed in the section on subject access requests), would help to alleviate potential costs (time and resource) in responding to these requests?

Somewhat Agree

#### Q2.3.3a. Please explain your answer, and provide supporting evidence where possible, including on:

#### Which safeguards should apply (such as mirroring Section 16 of the Freedom of Information Act (for public bodies) to help data subjects by providing advice and assistance to avoid discrimination)

#### What a reasonable cost limit would look like, and whether a different (i.e. sliding scale) threshold depending on the size (based on number of employees and/or turnover, for example) would be advantageous

This approach would be beneficial in limiting abuse of the right from those who potentially wish to cause a burden on the organisation and may support organisations in reducing the costs in handling large and complex requests. However, this approach may restrict access to those who have a genuine wish to access large volumes of complex information such as care leavers accessing their local authority records. If this proposal goes ahead, we think that in this specific example either life story work for care leavers would need to be improved or potentially exempt care leavers from this cost limit, as well as wider local authority social care files covering both adults and children.

### Q2.3.4. To what extent do you agree with the following statement: ‘There is a case for re-introducing a small nominal fee for processing subject access requests (akin to the approach in the Data Protection Act 1998)’?

Somewhat Disagree

#### Q2.3.4a. Please explain your answer, and provide supporting evidence where possible, including what a reasonable level of the fee would be, and which safeguards should apply.

Although reintroducing a fee may dissuade those without a genuine desire or purpose for accessing their data from making requests, we are in general not in favour of reintroducing a fee.

The re-introduction of a nominal fee would create a burden on organisations to ensure mechanisms are in place for the collection of payment. Furthermore, the only purpose would be seen as a method of encouraging individuals not to access the right and reverse the key principle of the right of access. If a fee were introduced it would be necessary to introduce exemptions where it would be a financial burden to the individual, which would be difficult to implement.

### Q2.3.5. Are there any alternative options you would consider to reduce the costs and time taken to respond to subject access requests?

Yes

#### Q2.3.5a. Please explain your answer and provide supporting evidence where possible.

Factor in need for requests to be specific in nature and not focussed on all information held, or a fishing exercise. Perhaps the introduction of an exemption/widening of the para 22 schedule 3 DPA management information exemption to cover situations where applicants are on fishing expeditions to gain an advantage in private legal proceedings/ongoing disputes, so that they request information through due processes and not through SARs.

In addition, remove social care records from the data subject rights and manage access to these under a separate regime similar to Access to Health Records.

## 2.4 Privacy and electronic communications

### Q2.4.1. What types of data collection or other processing activities by cookies and other similar technologies should fall under the definition of 'analytics'?

We do not have enough expertise of analytics to make an informed view.

### Q2.4.2. To what extent do you agree with the proposal to remove the consent requirement for analytics cookies and other similar technologies covered by Regulation 6 of PECR?

Neither Agree nor Disagree

#### Q2.4.2a. Please explain your choice, and provide supporting evidence where possible, including what safeguards should apply.

Participants in our Greater Manchester discussion on the proposals felt that the cookie consent was not something people were aware of the impact of – the public and some of the information governance experts were not aware of the infrastructure and functionality of cookies and how they process personal data.

There was also a feeling that the advertising industry would find ways to bypass the requirement for cookie consent by implementing other technology.

It was also reflected that the public, and many organisations consider cookie consent to be a requirement introduced by GDPR when in fact this was a requirement introduced by the Privacy and Electronic Communication Regulations 2003.

However, we also feel it is important that care should be taken to ensure that any analytics cookies which involve tracking a user’s behaviour or browsing history should only be used with the consent of the individual.

### Q2.4.3. To what extent do you agree with what the Government is considering in relation to removing consent requirements in a wider range of circumstances? Such circumstances might include, for example, those in which the controller can demonstrate a legitimate interest for processing the data, such as for the purposes of detecting technical faults or enabling use of video or other enhanced functionality on websites.

Somewhat Agree

#### Q2.4.3a. Please explain your answer, and provide supporting evidence where possible, including what circumstances should be in scope and what, if any, further safeguards should apply.

We agree with proposals to simplify and reduce requirements around cookies that would benefit users, and can see the logic in this but have a slight concern that there is a risk that it could be abused; what safeguards would be in place to prevent further data being collected? However, cookies which are essential for the functioning of the website should not require consent as true consent cannot be captured as there is no choice.

### Q2.4.4. To what extent do you agree that the requirement for prior consent should be removed for all types of cookies?

Strongly Disagree

#### Q2.4.4a. Please explain your answer and provide supporting evidence where possible. Please explain how organisations could comply with the UK GDPR principles on lawfulness, fairness and transparency if PECR requirements for consent to all cookies were removed.

The data subject needs to be able to have some element of control in this area. Individuals should be able to refuse consent to things like tracking cookies, and whilst personalised adverts can be seen as a benefit in that you aren’t seeing things that are irrelevant to you, not everyone wants to be the subject of targeted advertising and comparatively this benefits organisations commercially more than individuals. However, the requirement to consent to essential cookies should be removed.

### **Q2.4.5. Could sectoral codes (see Article 40 of the UK GDPR) or regulatory guidance be helpful in setting out the circumstances in which information can be accessed on, or saved to a user’s terminal equipment?**

Yes, a Code of Practice would be helpful in providing clear guidance.

### **Q2.4.6. What are the benefits and risks of requiring websites or services to respect preferences with respect to consent set by individuals through their browser, software applications, or device settings?**

Benefits –better data protection, increased public trust, increase in traffic/uptake of services, better individual outcomes

Risk – potential loss of advertising revenue if individuals don’t consent to tracking cookies, Risk of individuals getting frustrated and going elsewhere

### Q2.4.7. How could technological solutions, such as browser technology, help to reduce the volume of cookie banners in the future?

Whilst this is not our area of expertise, we understand that it is possible for an HTTP standard to communicate directly with the web server hosting a site being visited or communicate with the website itself and allow an individual to express their preference once and for that to be communicated going forward.

### Q2.4.8. What, if any, other measures would help solve the issues outlined in this section?

We have no further suggestions to make.

### Opt-in definition.

### Under PECR, Businesses can generally only contact individuals who have previously been in touch during a sale or transaction and have not refused or opted out of receiving marketing communications about similar products. This is known as a ‘soft opt-in’.

### Q2.4.9. To what extent do you agree that the soft opt-in should be extended to non-commercial organisations?

Somewhat Agree

Q2.4.9a. Please explain your answer and provide supporting evidence where possible.

Providing that the same requirements for the soft opt-in that are in place currently apply then it could benefit charities and increase political engagement for example.

### Q2.4.10. What are the benefits and risks of updating the ICO’s enforcement powers so that they can take action against organisations for the number of unsolicited direct marketing calls ‘sent’?

### Currently the ICO can only take action on calls which are ‘received’ and connected. The ICO sometimes receives intelligence of companies sending thousands of calls but which are not all connected, but they cannot take account of the potential risk of harm when determining the most appropriate form of enforcement action.

We agree with this proposal.

Benefits - It may deter organisations from making nuisance calls, encourage better practice, prevent fraud

Risks – may drive may organisations to operate from overseas and result in more poor handling of personal data

### Q2.4.11. What are the benefits and risks of introducing a ‘duty to report’ on communication service providers?

### This duty would require communication service providers to inform the ICO when they have identified suspicious traffic transiting their networks. Currently the ICO must rely on receiving complaints from users before they can request relevant information from communication service providers.

### Please provide information on potential cost implications for the telecoms sector of any new reporting requirements.

We agree that communication service providers should do all that they can to prevent fraud and nuisance calls.

Benefits – this would highlight non-compliance without increased burden on the regulator, may prevent fraud and encourage better practice, deter organisations from making nuisance calls.

Risk – would there be an unfair burden on communications providers to monitor, or liability if they didn’t?

We are unable to comment on potential cost implications.

### **Q2.4.12. What, if any, other measures would help to reduce the number of unsolicited direct marketing calls and text messages and fraudulent calls and text messages?**

* Stricter enforcement regime including monetary penalties, [measures set out in this plan such as authentication of CLI data, intelligence sharing, collaboration through working group and internationally](https://www.ofcom.org.uk/__data/assets/pdf_file/0025/216439/nuisance-calls-joint-action-plan-2021.pdf).
* More publicity – we feel that many people don’t know to report to ICO

### **Q2.4.13. Do you see a case for legislative measures to combat nuisance calls?**

Don’t Know.

Q2.4.13a. If yes, what measures do you propose and why? If no, please explain your answer, and provide supporting evidence where possible.

We can see a case for legislation being introduced, however, legislative measures are already in place such as PECR and we are not sure what more could be introduced. It may be better to strengthen the enforcement options available to the ICO such as increasing the level of monetary penalties which may be issued.

### Q2.4.14. What are the benefits and risks of mandating communications providers to do more to block calls and texts at source?

Same as Q2.4.11 above

### Q2.4.15. What are the benefits and risks of providing free of charge services that block, where technically feasible, incoming calls from numbers not on an ‘allow list’? An “allow list” is a list of approved numbers that a phone will only accept incoming calls from.

We do not feel there is enough information in consultation paper around what this would entail.

Benefits – may prevent fraud and protect individuals from distress/annoyance from nuisance calls

Risks – may be unfair on legitimate new businesses, what would the process be to be added to the allow list – could this add an administrative burden to the regulator?

It would be useful to have a list that legitimate businesses can sign up to, after having provided evidence of lawful processing and commitment to adherence of PECR principles, without too much financial burden on small businesses.

### Q2.4.16. To what extent do you agree with increasing fines that can be imposed under PECR so they are the same level as fines imposed under the UK GDPR (i.e. increasing the monetary penalty maximum from £500,000 to up to £17.5 million or 4% global turnover, whichever is higher)?

Strongly Agree

#### Q2.4.16a. Please explain your choice and provide supporting evidence where possible.

This would allow the ICO to fine accordingly based on aggravating and mitigating factors and may act as more of a deterrent. Organisations fined under the UK GDPR regime at present are often fined for actions which are the result of negligence or lack of due diligence, but organisations who have been fined under PECR have often wilfully ignored the TPS list or other rules and it does not seem fair that this more deliberate action should be fined less.

### Q2.4.17. To what extent do you agree with allowing the ICO to impose assessment notices on organisations suspected of infringements of PECR to allow organisations to carry out audits of the data controllers’ processing activities?

Strongly Agree

#### Q2.4.17a. Please explain your choice and provide supporting evidence where possible.

This would be a sensible approach and bring PECR enforcement into line with UK GDPR.

Q2.4.18. Are there any other measures that would help to ensure that PECR's enforcement regime is effective, proportionate and dissuasive?

Don’t Know

Q2.4.18a. If yes, what measures do you propose and why?

N/A

## 2.5 Use of personal data for the purposes of democratic engagement

Q2.5.1. To what extent do you think that communications sent for political campaigning purposes by registered parties should be covered by PECR’s rules on direct marketing, given the importance of democratic engagement to a healthy democracy?

Somewhat Disagree

#### Q2.5.1a. Please explain your answer and provide supporting evidence where possible.

Democratic engagement is important but receiving unwanted marketing from political parties could have the reverse effect.  Use of data is permitted for campaigning during elections, which allows raising awareness of parties and policies at the relevant time, so don’t see the benefit in this proposal.

### Q2.5.2. If you think political campaigning purposes should be covered by direct marketing rules, to what extent do you agree with the proposal to extend the soft opt-in to communications from political parties?

Somewhat Disagree

Q2.5.2a. Please explain your answer and provide supporting evidence where possible.

It was felt that marketing undertaken by political parties was too easy to manipulate to push out particular message and increase division in politics and society. In addition, it was felt that the targeting of particular messages to specific groups stifles political debate and does not aid democracy since no one is receiving a full picture of parties’ policies.

Transparency of messages and fact checking is required to combat the spread of disinformation, particularly through social media, and allowing targeted marketing does not allow for this to happen.

### Q2.5.3. To what extent do you agree that the soft opt-in should be extended to other political entities, such as candidates and third-party campaign groups registered with the Electoral Commission?

Somewhat Disagree

#### Q2.5.3a. Please explain your answer and provide supporting evidence where possible.

As above, care needs to be taken to ensure any marketing undertaken is transparent and fact checked, which is not possible if marketing is targeted at specific individuals.

### Q2.5.4. To what extent do you think the lawful grounds under Article 6 of the UK GDPR impede the use of personal data for the purposes of democratic engagement?

Somewhat Disagree

#### Q2.5.4a. Please explain your answer and provide supporting evidence where possible.

The legislation allows for legitimate use of personal data at necessary times such as elections and safeguards inappropriate use of data at other times.

### Q2.5.5. To what extent do you think the provisions in paragraphs 22 and 23 of Schedule 1 to the DPA 2018 impede the use of sensitive data by political parties or elected representatives where necessary for the purposes of democratic engagement?

Somewhat Disagree

#### Q2.5.5a. Please explain your answer and provide supporting evidence where possible.

The legislation allows for legitimate use of personal data at necessary times such as elections and safeguards inappropriate use of data at other times.

## 2.6 Further questions

### Q2.6.1. In your view, which, if any, of the proposals in ‘Reducing Burdens on Businesses and Delivering Better Outcomes for People’, would impact on people who identify with the protected characteristics under the Equality Act 2010 (i.e. age, disability, gender reassignment, marriage and civil partnership, pregnancy and maternity, race, religion or belief, sex and sexual orientation)?

SAR proposals would likely impact on people who identify with protected characteristics under the Equality Act 2010. Care leavers or individuals seeking recourse to public funds may be disadvantaged if charges are introduced for SAR requests or a costs or time threshold is implemented, akin to the FOI. This could be mitigated by exempting certain categories of individuals from the fee regime

Impact would otherwise be largely positive

### Q2.6.2. In addition to any of the reforms already proposed in ‘Reducing burdens on business and delivering better outcomes for people’, (or elsewhere in the consultation), what reforms do you think would be helpful to reduce burdens on businesses and deliver better outcomes for people?

We have no further suggestions to add. As has been noted in a number of our responses to the questions in this consultation, perceived burdens could be alleviated by providing clear guidance and advertising their existence widely.

### Q2.6.3. In addition, the Government would welcome views on the desirability of consolidating the UK GDPR and the Data Protection Act 2018.

We believe this would be very helpful for data subjects and organisations as well as professionals working within data protection roles.

End of chapter Q. Do you have any general comments about this chapter not yet captured by your responses to the questions above?

Under the Data Protection Act 1998 there were definitions used when more than one data controller is involved in processing which reflected different kinds of relationship. In the current UK GDPR and DPA only one, Joint Data Controllers remains, and this is where two organisations are clearly working jointly together on the data processing.

The term which has been removed from the legislation is Data Controllers “In Common” where individual data controllers are all working together for a common purpose but are acting separately rather than jointly to decide the manner of processing. For example, in the work around health and social care share care records, the term being proposed for use is “joint data controllers”. However, in reality this is not the case, since one organisation is determining the manner of processing, whilst the other data controllers are working on the common purpose for processing. This would help to clarify the types of governance arrangements and agreements (both legal and good practice) that are required.

Another example of data controllers “In Common” rather than joint data controllers is where an organisation has a statutory duty to provide a service, and they procure a provider to do that on their behalf where the provider is making their own decisions about the purpose and manner of processing that the commissioning authority has no involvement in. Having a statutory duty makes the commissioner a data controller, but the parties are both acting independently with a “common” goal/purpose.